UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
premises located at 1227 E. Walnut Street, Unit 3, Green Bay, Wisconsin, ("PREMISES"); vehicle identified as a 2021 silver Jeep Gladiator pick-up truck (bearing Wisconsin plate no. VC1762) ("Subject Vehicle"); the person of Elias RUIZ (H/M, DOB XX/XX/1979)

Case No. 24 MJ 220

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please see Attachment A.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 922(d)	Transferring a Firearm to a Prohibited Person
18 U.S.C. § 922(o)	Possession of a Machine Gun
18 U.S.C. § 371	Conspiracy

The application is based on these facts:

Please see Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Sean Carlson, Special Agent - ATF
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 10/18/2024

Judge's signature

City and state: Milwaukee, WI

Honorable William E. Duffin, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF
APPLICATIONS FOR SEARCH WARRANTS

I, Sean Carlson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the premises located at 1227 E. Walnut Street, Unit 3, Green Bay, Wisconsin, ("PREMISES"), further described in Attachment A (collectively, "Attachment A"); the vehicle identified as a 2021 silver Jeep Gladiator pick-up truck (bearing Wisconsin plate no. VC1762) (hereinafter referred to as the "Subject Vehicle"); and the person of Elias RUIZ (H/M, DOB XX/XX/1979), for the things described in Attachment B.

2. I am employed as a Special Agent with the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") assigned to the Milwaukee Field Office since November 2015. I have been employed as a full-time law enforcement officer for approximately fifteen years. Prior to my employment at ATF, I was a Patrol Officer at the Hammond Police Department in Hammond, Indiana for over four (4) years, and then I served approximately five (5) years as a Federal Air Marshal with the U.S. Department of Homeland Security.

3. As a Special Agent, I have participated in the investigation of firearms and narcotics-related offenses, resulting in the prosecution and conviction of numerous individuals and the seizure of illegal drugs, and weapons. As a firearms investigator, I have interviewed many individuals involved in firearm and drug trafficking and have obtained information from them regarding acquisition, sale, importation, manufacture, and distribution of firearms and controlled substances. Through my training and experience, I am familiar with the actions, habits, traits,

methods, and terminology utilized by the traffickers and abusers of controlled substances.

4. Based on my training, experience and participation in drug trafficking and firearms trafficking investigations, I know and have observed the following:

a. I have relied on informants to investigate firearms trafficking and drug trafficking. Through informant interviews and debriefings of individuals involved in those offenses, I have learned about the manner in which individuals and organizations finance, purchase, transport, and distribute firearms and narcotics both within and outside of Wisconsin. I have utilized informants to conduct "controlled purchases" of firearms and controlled substances from individuals, as opposed to licensed gun dealers. I have also conducted surveillance of individuals engaged in firearms and drug trafficking and participated in the execution of numerous search warrants resulting in the seizure of drugs, firearms, ammunition, and magazines.

b. Based on my training and experience, I have become familiar with the language utilized over the telephone to discuss firearms and drug trafficking and know that the language is often limited, guarded, and coded. I also know that firearms and drug traffickers often use electronic devices (such as computers and cellular phones) and social media to facilitate these crimes. Based on my experience, I know that firearms traffickers may keep photographs of these items on electronic devices.

c. I also know that drug traffickers and firearms traffickers commonly possess—on

their person, at their residences, at their places of business, in their vehicles, and other locations where they exercise dominion and control—firearms, ammunition, and records or receipts pertaining to such.

d. I know that firearms traffickers and drug traffickers often put their telephones in nominee names to distance themselves from telephones that are utilized to facilitate these and related offenses. I also know that firearm and drug traffickers often use proceeds to purchase assets such as vehicles, property, jewelry, and narcotics. I also know that firearm and drug traffickers often use nominees to purchase or title these assets to avoid scrutiny from law enforcement.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other investigators and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

6. There is probable cause to believe that evidence of violations of the following laws of the United States, including the things described in Attachment B, will be found in the property listed in Attachments A, respectively: 18 U.S.C. § 922(d) (transferring a firearm to a prohibited person), 18 U.S.C. § 922(o) (possession of a machine gun), and 18 U.S.C. § 371 (conspiracy).

PROBABLE CAUSE

7. On February 1, 2022, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), Special Agent (SA) Sean Carlson and Brown County Sheriff's Officer (Ofc.) Al Wysocki

debriefed ATF Confidential Informant no. 30939 (CI 30939). CI 30939 stated to investigators a black male known to them by the nickname "BUMP" or "BUMPY" was selling large amounts of firearms utilizing Facebook messenger. CI explained they are contacted on a near weekly basis by "BUMPY" with new firearms that are available to purchase. CI 30939 stated he/she has known "BUMPY" for approximately four (4) years and has purchased firearms from him in the past. CI 30939 provided investigators with the Facebook account "BUMPY JOHNSON (Facebook Username BUMPY JOHNSON, Facebook ID 100042803601377)," which BUMPY JOHNSON uses to communicate for all his potential firearms dealings.

8. CI 30939 stated BUMPY acquires his firearms from an unknown Mexican male who drives a burnt orange Dodge Charger sedan and operates near a Mexican grocery store in Green Bay, Wisconsin. CI 30939 further explained the unknown Mexican male gets the firearms from a source in Minnesota who steals them from trains. CI 30939 explained the firearms are usually in pristine unused condition, still inside the manufacturer's packaging.

9. It should be noted, CI 30939 is providing information to law enforcement in hopes to garner judicial consideration for a pending Wisconsin charge of possession with intent to distribute Fentanyl. CI 30939 has previously been convicted of Armed Robbery, possession of THC, possession of a stolen vehicle (three times), and possession of a controlled substance (two times). Investigators believe the information provided by CI 30939 to be truthful and credible based on Facebook photos from private conversations CI 30939 has provided to investigators that has been able to be corroborated. Additionally, CI 30939 has previously provided narcotics related

information to Brown County Sheriff's Officer Al Wysocki that he was able to corroborate through separate investigation. CI 30939 was actively cooperating with law enforcement and participated in a February 2022 recorded controlled buy of a firearm where Jeremy JOHNSON was the target. As of 2024, following the controlled purchase from JOHNSON in 2022, CI 30939 chose to end their cooperation with law enforcement and his left the Wisconsin Area.

10. Prior to this meeting with CI 30939, Ofc. Wysocki had previously identified "BUMPY JOHNSON" as Jeremy Roman JOHNSON (B/M, DOB XX/XX/1991). JOHNSON was identified via a booking photograph. It should be noted, a search of JOHNSON's criminal history reveals he is a convicted felon, having prior state convictions for Robbery (2009) and Burglary (2009).

ELIAS RUIZ AND CELLPHONE NUMBER 956-590-9670

11. On March 15, 2022, the Honorable William E. Duffin, U.S. Magistrate judge, signed a search warrant for the data associated with the Facebook account BUMPY JOHNSON (Facebook Username BUMPY JOHNSON, Facebook ID 100042803601377).

12. On March 22, 2022, Your Affiant conducted a search of common law enforcement databases and located the phone number 956-590-9670 as belonging to RUIZ. On that same date, Your Affiant submitted a grand jury subpoena to AT&T, the owner of Cricket Wireless, for toll records and subscriber information pertaining to this phone number.

13. On April 19, 2022, Your Affiant reviewed data for the Facebook account BUMPY JOHNSON (Facebook Username BUMPY JOHNSON, Facebook ID 100042803601377),

provided by Facebook pursuant to the aforementioned Federal search warrant signed on March 15, 2022. Your Affiant located conversation, which occurred on April 25, 2021, between JOHNSON and an unknown male using the Facebook Account "REYNALDO ESTUPINIAN," in which REYNALDO ESTUPINIAN is advertising two (2) firearms he is selling.

14. On the same date, REYNALDO ESTUPINIAN sent JOHNSON a screenshot from a cellular phone's text message conversation. The screenshot appears to depict a conversation the user of the profile REYNALDO ESTUPINIAN is having with a contact he has labeled as "ELIAS RUIZ." The conversation includes smaller photographs of the two (2) firearms depicted above and contains several apparent prices for the firearms. Based on this conversation Your Affiant believes that for these particular firearms, the owner of the Facebook profile REYNALDO ESTUPINIAN is buying firearms from ELIAS RUIZ and reselling them to JOHNSON. The screenshot depicts ELIAS RUIZ's cellular phone number as 956-590-9670. It should be noted, this phone number is the same as the phone number Your Affiant previously identified as being associated with RUIZ.

15. On April 26, 2022, Your Affiant reviewed Cricket Wireless subscriber information for 956-590-9670 obtained through Grand Jury Subpoena served on March 22, 2022. Cricket Wireless lists the subscriber of this number as Elias RUIZ. Cricket Wireless further states this account was activated on August 09, 2015, and it remains active as of May 02, 2022.

Search Warrant and Interview of Elias RUIZ

16. On July 06, 2022, personnel from the ATF executed a federal search warrant at the

1227 E. Walnut Street, Unit 3, Green Bay, Wisconsin (PREMISES). During the execution of the warrant, RUIZ was present and interviewed by your Affiant. During the search of the residence, agents located and seized the following items of evidence; eleven (11) firearms (nine (9) pistols and two (2) rifles), approximately 2046 rounds of misc. caliber ammunition, six (6) firearms manufacturer boxes, two cellular phones, two firearms purchase documents for purchases made by RUIZ, and items of indicia of residency for RUIZ at the PREMISIS. It should be noted, the six firearms boxes contained serial numbers for firearms that were NOT located at the residence during the execution of the warrant.

17. While agents were processing the scene, your affiant, ATF SA Luke Barker and Brown County Sheriff's Office (BCSO) Detective Al Wysocki conducted a recorded interview of RUIZ.

18. RUIZ stated he owned several firearms and described where they would be found throughout the residence. When asked where he gets his firearms, RUIZ stated he purchased his firearms from gun shows and stated he "buys and sells". Your affiant asked how long he has been selling firearms, and RUIZ stated, "about a year, until it got slow". RUIZ further explained he started buying firearms as collectibles, and after a while he started selling more and more frequently. When asked why he was selling firearms, RUIZ started selling firearms in order "to make extra money." RUIZ stated he did not typically purchase his firearms from Federal Firearms Licensees (FFL), and instead purchased firearms via private sale at gun shows. Your affiant asked RUIZ how many firearms he has bought and sold over the year, and RUIZ replied "A lot. I used

to buy probably four or five guns per show."

19. RUIZ explained that when he would purchase a firearm, for the purpose of resale, he would mark up the pistol in order to make a profit. In one specific example, RUIZ stated if he purchased a firearm for $400, he would mark it up and resell it for at least $600. RUIZ explained he would take orders for specific firearms prior to going to the gun shows. RUIZ stated he had approximately 3 or 4 additional customers to whom he regularly sells firearms. During the interview, RUIZ outlined selling the two firearms, which ATF purchased from RUIZ and JOHNSON, on February 28, 2022, via a controlled purchase. RUIZ stated he purchased these firearms at a gun show in Milwaukee, which was later confirmed to be accurate via an ATF eTrace report. RUIZ also outlined the sales of four or five firearms to a subject he identified as "Jose FIGEROA". RUIZ stated he knew FIGEROA was not a US citizen.

20. To conclude the interview, your affiant explained to RUIZ that his repetitive purchase of firearms for resale was a violation of federal law. Additionally, your affiant advised him it was illegal to buy firearms for felons, and if he was in fact a convicted felon, it would be illegal for him to possess firearms as well. RUIZ stated he understood.

September 2024 – RUIZ firearm recovery by Brown County Sheriff's Office

21. On September 13, 2024, Brown County Sheriff's Office (BCSO) executed a State of Wisconsin search warrant for 249 Victoria Street, Green Bay, Wisconsin, related to an on-going narcotics investigation. During the search of the residence, officers located a tan and black, Smith & Wesson pistol (9mm, model SD9, serial no. FEJ1102). BCSO investigators traced the firearm

and learned that it was sold to a James D. KOTKE (DOB 05/25/1971) on September 5, 2024, at The Pawn Shop, located at 219 N. Main Street, Oconto Falls, Wisconsin.

22. On September 17, 2024, BCSO investigator Shields interviewed KOTKE, who stated he sold the firearm on September 7, 2024. KOTKE stated he sold the firearm to "Elias RUIZ", at a gun show being operated at Jeff's Sports Bar and Grill, located at 6010 County Road D, Kewaunee Wisconsin. KOTKE provided investigators RUIZ's phone number as (956) 590-9670, and stated he knew that RUIZ currently resided at 1227 Walnut Street, Unit 3, Green Bay, WI (PREMISIS). Investigators texted KOTKE a 2016 booking photograph of RUIZ but KOTKE could not positively identify RUIZ from the photograph, however, he described RUIZ as a Hispanic male, approximately 5'08" tall and weighing approximately 220 pounds, with scruffy facial hair. Your affiant is aware that description is consistent with the appearance of Elias RUIZ. KOTKE stated, at one point after the sale, he had a physical document with RUIZ's information written on it, but he no longer had that paper. BCSO investigators later spoke to the staff of Jeff's Sports Bar and Grill and confirmed that there was a gun show at this location on September 7, 2024, which is consistent with KOTKE's statement. BCSO investigators obtained surveillance footage from the business which depicted a portion of the parking lot. BCSO investigators observed a silver Jeep Gladiator pick up truck drive through the lot and park out of view. A short time later, investigators observed this vehicle leave the lot. Your affiant is aware that RUIZ is the registered owner of a silver Jeep Gladiator pick-up truck.

23. On October 02, 2024, ATF SA Brad Kurtzweil conducted surveillance at 1227 E.

Walnut Street, Unit 3, Green Bay, WI (PREMISES). Prior to conducting surveillance, SA Kurtzweil reviewed photos of RUIZ. Also, SA Kurtzweil has previously had contact with RUIZ during the 2022 execution of a search warrant at RUIZ's residence. At approximately 11:55 AM CST, SA Kurtzweil observed RUIZ exit the door to apartment 3 and enter a silver Jeep Gladiator pick-up truck (2021, bearing Wisconsin License Plate no. VC1762). RUIZ then drove away from the residence. It should be noted, this vehicle is registered to RUIZ at the PREMISES.

CONCLUSION

24. Your Affiant is aware through training and experience that it is common for those who possess and traffic firearms, to utilize electronic media devices, which often possess cameras, to photograph and send messages to negotiate the purchase and sale of their firearms. Your Affiant is also aware that firearms are a commodity that are often held for long periods of time. As stated above, in 2024, after being advised that it was illegal to purchase and resell firearms for profit, RUIZ seemingly purchased a firearm at a gun show, on September 7, 2024, which was recovered by law enforcement on September 13, 2024. Your Affiant knows from training and experience, this very short time between RUIZ acquiring the firearm and transferring it again, is consistent with someone who is engaged in firearms trafficking. Additionally, the pattern of this purchase is consistent with RUIZ's own statements to ATF in 2022.

TECHNICAL TERMS

25. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

26. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

27. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

i. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via

the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

ii. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

iii. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

iv. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

28. *Forensic evidence.* As further described in Attachment B, these applications seek permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

i. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of

information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

ii. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device

connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

iii. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

iv. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrants.

v. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

29. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the

warrants. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

i. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrants call for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrants can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

ii. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

iii. Variety of forms of electronic media. Records sought under these warrants could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

31. Because several people share the PREMISES listed in Attachments A, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in these warrants could be found on any of those computers or storage media, the warrants applied for would permit the seizure and review of those items as well.

CONCLUSION

32. I submit that this affidavit supports probable cause for warrants to search the PREMISES described in Attachments A, and seize the items described in Attachment B.

ATTACHMENT A
Property to be searched

1. The person of Elias RUIZ (H/M, DOB XX/XX/1979)

2. The vehicle identified as a 2021 silver Jeep Gladiator pick-up truck (bearing Wisconsin plate no. VC1762, registered to RUIZ)

3. The property to be searched is the premises located at 1227 E. Walnut Street, Unit 3, Green Bay, Wisconsin, any additional on-site storage units, or standalone garage storage that is provided to the residents of Unit 3. The building is white two-story apartment building with individual entrances for each unit located on the ground level directly off the driveway. See the below photograph depicting the PREMISES.

ATTACHMENT B

Property to be seized

All records relating to violations of 18 U.S.C. § 922(d) (transferring a firearm to a prohibited person), 18 U.S.C. § 922(o) (possession of a machine gun) and 18 U.S.C. § 371 (conspiracy), involving Elias Ruiz, Reynaldo ESTUPINIAN, and Jeremy JOHNSON

1. Firearms

2. Agents may document any tattoos on RUIZ's hands and arms

3. Documents or information related to the purchase and/or sale of firearms, ammunition, firearms accessories;

4. Photographs or other documents related to firearms, ammunition, firearms accessories;

5. ATF Form 4473s, firearms, firearm boxes, bipods, tripods, upper receivers, receipts and any records related to firearms, firearms accessories, ammunition, financial documents that transfer of proceeds of the above schemes, computers, electronics capable of communication, and cellphones such as:

   a. lists of contacts and any identifying information;

   b. photographs, videos, or other media storage connected to firearms;

   c. types, amounts, and prices of firearms purchased/sold;

   d. any information related to sources or purchasers of firearms (including names, addresses, phone numbers, or any other identifying information);

   e. all bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;

f. any and all financial records connected to the purchase/sale of firearms;

6. Cellphones, computers, and all media storage devices that may hold documentation regarding firearm or ammunition purchases/sales and customers;

7. Any and all financial records connected to the purchase/sale of firearms, and any correspondence between suspects and other firearms sellers and/or purchasers;

8. All bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;

9. Proceeds of firearms trafficking activities, including United States currency;

10. All bank records, checks, credit card bills, account information, and other financial records; Financial records, documents, statements, or other evidence of control of bank or other financial accounts and investment funds;

11. Personal address books, telephone bills, photographs, letters, personal notes, documents and other items or lists reflecting names, addresses, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in firearms trafficking activities;

12. Documents and deeds reflecting the purchase or lease of items obtained with the proceeds from firearm trafficking activities;

13. Records of off-site locations to store proceeds and other records, including safes, vaults, or lock boxes, safe deposit box keys, records and receipts and rental agreements for storage facilities;

14. Records of mail and communications services, cellular telephones and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text

messages, digital audio and or video recordings, pictures, settings, and any other user defined settings and/or data;

15. Indicia of occupancy, residency or ownership of the premises, including utility bills, telephone bills, loan payment receipts, addressed envelopes, escrow documents and keys;

16. Indicia of occupancy, residency, rental, ownership, or use of the Subject Premises and any vehicles found thereon during the execution of the warrant, including paid utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, identification documents, keys, records of real estate transactions, vehicle titles and registration, and vehicle maintenance records; Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

17. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

18. All records relating to violations of 18 U.S.C. § 922(d) (transferring a firearm to a prohibited person), 18 U.S.C. § 922(o) (possession of a machine gun) and 18 U.S.C. § 371 (conspiracy), involving Elias Ruiz, Reynaldo ESTUPINIAN, and Jeremy JOHNSON:

a. Records and information relating to a conspiracy to violate the laws of the United States, including the scope, manner, means, acts in furtherance, and identity of any co-conspirators;

b. Records and information relating to the identity or location of the suspects;

c. Records and information relating to communications with Internet Protocol addresses;

d. Records and information relating to the crimes referenced in Attachment B, paragraph 14; and

e. Records and information relating to intent or state of mind.

19. Computers or storage media used as a means to commit the violations described above;

20. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

21. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

22. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

23. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the ATF may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

☑ Original [illegible]

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
premises located at 1227 E. Walnut Street, Unit 3, Green Bay, Wisconsin, ("PREMISES"); vehicle identified as a 2021 silver Jeep Gladiator pick-up truck (bearing Wisconsin plate no. VC1762) ("Subject Vehicle"); the person of Elias RUIZ (H/M, DOB XX/XX/1979)

Case No. 24 MJ 220

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

Please see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Please see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 11/01/2024 *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable William E. Duffin.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 10/18/2024 at 1:40 p.m.

William E. Duffin
Judge's signature

City and state: Milwaukee, WI

Honorable William E. Duffin, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A
Property to be searched

1. The person of Elias RUIZ (H/M, DOB XX/XX/1979)

2. The vehicle identified as a 2021 silver Jeep Gladiator pick-up truck (bearing Wisconsin plate no. VC1762, registered to RUIZ)

3. The property to be searched is the premises located at 1227 E. Walnut Street, Unit 3, Green Bay, Wisconsin, any additional on-site storage units, or standalone garage storage that is provided to the residents of Unit 3. The building is white two-story apartment building with individual entrances for each unit located on the ground level directly off the driveway. See the below photograph depicting the PREMISES.

ATTACHMENT B

Property to be seized

All records relating to violations of 18 U.S.C. § 922(d) (transferring a firearm to a prohibited person), 18 U.S.C. § 922(o) (possession of a machine gun) and 18 U.S.C. § 371 (conspiracy), involving Elias Ruiz, Reynaldo ESTUPINIAN, and Jeremy JOHNSON

1. Firearms

2. Agents may document any tattoos on RUIZ's hands and arms

3. Documents or information related to the purchase and/or sale of firearms, ammunition, firearms accessories;

4. Photographs or other documents related to firearms, ammunition, firearms accessories;

5. ATF Form 4473s, firearms, firearm boxes, bipods, tripods, upper receivers, receipts and any records related to firearms, firearms accessories, ammunition, financial documents that transfer of proceeds of the above schemes, computers, electronics capable of communication, and cellphones such as:

   a. lists of contacts and any identifying information;

   b. photographs, videos, or other media storage connected to firearms;

   c. types, amounts, and prices of firearms purchased/sold;

   d. any information related to sources or purchasers of firearms (including names, addresses, phone numbers, or any other identifying information);

   e. all bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;

f. any and all financial records connected to the purchase/sale of firearms;

6. Cellphones, computers, and all media storage devices that may hold documentation regarding firearm or ammunition purchases/sales and customers;

7. Any and all financial records connected to the purchase/sale of firearms, and any correspondence between suspects and other firearms sellers and/or purchasers;

8. All bank records, checks, credit card bills, account information, and other financial records related to firearms commerce;

9. Proceeds of firearms trafficking activities, including United States currency;

10. All bank records, checks, credit card bills, account information, and other financial records; Financial records, documents, statements, or other evidence of control of bank or other financial accounts and investment funds;

11. Personal address books, telephone bills, photographs, letters, personal notes, documents and other items or lists reflecting names, addresses, telephone numbers, addresses and communications regarding illegal activities among and between members and associates involved in firearms trafficking activities;

12. Documents and deeds reflecting the purchase or lease of items obtained with the proceeds from firearm trafficking activities;

13. Records of off-site locations to store proceeds and other records, including safes, vaults, or lock boxes, safe deposit box keys, records and receipts and rental agreements for storage facilities;

14. Records of mail and communications services, cellular telephones and all electronic storage areas on the device including stored telephone numbers, recently called numbers list, text

messages, digital audio and or video recordings, pictures, settings, and any other user defined settings and/or data;

15. Indicia of occupancy, residency or ownership of the premises, including utility bills, telephone bills, loan payment receipts, addressed envelopes, escrow documents and keys;

16. Indicia of occupancy, residency, rental, ownership, or use of the Subject Premises and any vehicles found thereon during the execution of the warrant, including paid utility and telephone bills, canceled envelopes, rental, purchase or lease agreements, identification documents, keys, records of real estate transactions, vehicle titles and registration, and vehicle maintenance records; Evidence of user attribution showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

17. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

18. All records relating to violations of 18 U.S.C. § 922(d) (transferring a firearm to a prohibited person), 18 U.S.C. § 922(o) (possession of a machine gun) and 18 U.S.C. § 371 (conspiracy), involving Elias Ruiz, Reynaldo ESTUPINIAN, and Jeremy JOHNSON:

a. Records and information relating to a conspiracy to violate the laws of the United States, including the scope, manner, means, acts in furtherance, and identity of any co-conspirators;

b. Records and information relating to the identity or location of the suspects;

c. Records and information relating to communications with Internet Protocol addresses;

d. Records and information relating to the crimes referenced in Attachment B, paragraph 14; and

e. Records and information relating to intent or state of mind.

19. Computers or storage media used as a means to commit the violations described above;

20. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

21. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

22. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

23. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the ATF may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.